PayPoint Gateway Overview
NC Office of the State Controller
Revised February 15, 2010

What is the PayPoint Gateway?
PayPoint is a web capture gateway solution available from First Data Government Solutions (FDGS) through SunTrust Merchant Services (STMS). The service is an optional gateway service that may be subscribed to under OSC's master contract with STMS. PayPoint is different from the State's Common Payment Service gateway provided by ITS, as PayPoint offers a web "consumer interface" component and CPS does not.

What are the two primary payment processes offered by PayPoint?
PayPoint's consumer interface offers an agency the ability to accept online payments from citizens (consumers) and process them through one of two options. The option utilized depends upon who will authenticate the attempted payment, the agency or PayPoint. Under each option, the citizen accesses the agency's website first.
- Authentication performed by agency – Agency authenticates attempted payment to an internal database of open transactions, and if there is a match, the citizen is then redirected to PayPoint allowing him/her to select the payment method to complete the transaction.
- Authentication performed by Paypoint – From the agency's website, the citizen is redirected to a PayPoint hosted website, where the authentication process is performed against a database maintained at PayPoint, and if there is a match, the citizen can select the payment method to complete the transaction.

How is PayPoint made aware of the open transaction(s) for which a payment may be initiated?
This will depend upon who performs the authentication function, the agency or PayPoint.
- Authentication performed by agency – The HTTP QUERY String Web Service process is utilized. Upon a successful match, the agency passes the open transaction data to PayPoint, where the transaction can then be completed by citizen selecting his/her payment option. PayPoint does not retain or maintain a database of open transactions, as it only acts upon the single query string message submitted by the agency. The customer is then returned to the agency's website.
- Authentication performed by Paypoint – The Batch FTP process is utilized. The agency submits to PayPoint a file containing all open transactions though a Batch FTP upload process. The agency must keep the open transaction file updated in order for PayPoint to be able to authenticate attempted payments. PayPoint retains the open transaction in the database flagged as open until the transaction is either paid, or later deleted by the agency. Additionally, at anytime through the Admin feature, the agency can manually update the open transaction file in the database maintained at PayPoint (add or delete a transaction).

How is the agency made aware of successful payments initiated through PayPoint?
This will depend upon who performs the interfacing of open transactions utilized.
- HTTP QUERY String Web Service – PayPoint communicates back to the agency's return URL real time, upon either the success or failure of an attempted payment. This allows the agency to update its database of open transactions as payments are made at PayPoint. While pertinent transaction data is remitted to the agency, cardholder account data is retained by PayPoint.
- Batch FTP – Agency downloads a posting file, normally the next business day, either manually or via an automated process. The posting file contains data allowing the agency to update its open transactions file. This method does not provide the agency to ability to update its database of open transactions real time.

In both cases however, the agency can utilize PayPoint's Admin feature to ascertain the status of a payment at any time. In the case of the Batch FTP method, the agency can view the status of a transaction in the latest open transactions file submitted, as well as view the history of payments made. In the case of the

HTTP Query String method, since PayPoint does not maintain an open transaction database, the agency can only view the history of payments made.

Comparison of the two methods of transmitting open transaction data to PayPoint

Consultation with OSC and/or First Data and consideration of the agency's needs are required in order to select the appropriate method. The two methods are: 1) HTTP Query String Web Service; and 2) Batch FTP. Below is a comparison of the two methods associated with the <u>Consumer Interface feature</u>.

Comparison of Two Transmission Methods w/ Consumer Interface Feature					
Method	**Real Time**	**Authenti-cation**	**Agency's Role**	**Pros**	**Cons**
HTTP Query String Web Service	Yes	On Agency's website	Maintains agency website for authentication of A/R (invoice ID and amount) before being forwarded to PayPoint for selection of payment method Invoice data is transferred to Paypoint to be displayed to payor only when payor's online-entered data is authenticated by agency, thereby allowing payor to select payment method Agency receives response real-time from PayPoint when payment is authorized/rejected	Database of open transactions does not have to be maintained and be kept updated on PayPoint's servers Receipt of payment notification from PayPoint is real-time via returned query string	Agency has to develop web form to capture transaction on agency's website. Agency has to develop program to authenticate against agency maintained database, and if a match, submit query string to PayPoint.
Batch FTP	No	On PayPoint website	Create open A/R transaction file and upload to PayPoint, keeping database maintained at PayPoint updated Upload can be via auto FTP or through Admin site Agency's website has a link to PayPoint, where payor enters all payment data, resulting in PayPoint performing authentication based on open transactions database, and offering payment method to payor Files must be created in a format specific to the agency. Data encryption software must be used such as WinZip or others that are SSL 128 bit compatible.	No programming needed for agency authentication Receipt of payment notification can be real time, but only if an optional "Post Authorization plug-in" module is obtained (customization required)	Database at PayPoint must be maintained and kept updated. Requires Secure FTP upload, generally daily Receipt of payment notification from PayPoint not real-time, only when retrieval of posting file is downloaded, or transaction data viewed via Admin site

What features are available via the two PayPoint consumer upload interface options?

HTTP Query String Web Service				
Standard Features				**PayPoint Fee**
	Payment Gateway	Application hosted by First Data		$.20 / Trans
	Consumer Interface	Payments entered on PayPoint via Web		$.10 / Trans
	Database	On agency's website		N/A
	Authentication	On agency's website		N/A
	Portal Builder	Used by agency to design site		Included
	Admin Site	Used by agency to perform variety of functions		Included
	Virtual Terminal	Agency can key transactions via Admin site		Included
	Posting File	Downloadable (completed transactions)		Included
		Total Basic Fees Per Transaction		**$.30**
	For transactions entered via PayPoint's Admin site (Virtual Terminal), the $.10 per transaction fee does <u>not</u> apply.			
Optional Features				
	Summary Presentment	Not normally applicable under Query String		N/A
	Enrollment	Not normally applicable under Query String		N/A

Batch FTP				
Standard Features				**PayPoint Fee**
	Payment Gateway	Application hosted by First Data		$.20 / Trans
	Consumer Interface	Payments entered on PayPoint via Web		$.10 / Trans
	Database	On PayPoint's website		Included
	Authentication	On PayPoint's website		$.05
	Portal Builder	Used by agency to design site		Included
	Admin Site	Used by agency to perform variety of functions		Included
	Virtual Terminal	Agency can key transactions via Admin site		Included
	Posting File	Downloadable (completed transactions)		Included
		Total Basic Fees Per Transaction		**$.35**
	For transactions entered via PayPoint's Admin site (Virtual Terminal), the $.10 per transaction fee does <u>not</u> apply.			
Optional Features				
	Summary Presentment	Users can be displayed both unpaid and paid invoices. (With Enrollment feature, or if match of challenge data.)		$.10 / trans
	Enrollment	Users can be enrolled on PayPoint, allowing users' self-service to update user's profile, payment method(s), ability to view history of prior transactions, and to initiate reoccurring payments (if offered)		$.02 per enrollment
	Reoccurring	User can be setup to schedule payments to be auto-made against card or bank account on file		With enrollment only

What are the major features that distinguish PayPoint from the Common Payment Service?
- PayPoint has a consumer interface, which has a web capture feature as part of the solution.
- Multiple Payment Options – PayPoint allows the site visitor to select one of two payment options – credit/debit card or ACH bank draft (E-Check)

When is PayPoint suitable for an agency?
- Agency desires to accept payments online, but does not have the internal resources and/or expertise to develop a comprehensive in-house web capture application
- Agency desires to utilize a third-party gateway service provider to minimize (but not completely avoid) applicability of the PCI Data Security Standard requirements, primarily by avoiding the agency ever having to store cardholder data in the agency's database
- Agency desires to offer both the ACH bank draft payment option (E-Check), in addition to the card option
- Agency has outstanding invoices (accounts receivable transactions) associated with payors, which are conducive to being authenticated online-real time, either on the agency's website or on PayPoint's website, before being accepted and transacted via PayPoint.

Is PayPoint the gateway of choice for an agency needing gateway services?
OSC's policy states, "Agencies requiring a gateway service in order to participate in the MSA(s) may select either the Common Payment Service (CPS) gateway offered through ITS, or secure a gateway service of its choosing, provided it acquires approval from OSC and adheres to all applicable procurement requirements."

PayPoint is just one of several third-party gateways that an agency may elect to utilize, if the Common Payment Service does not meet the agency's needs. Some third-party gateways specialize in certain types of transactions that are more suitable for the agency. For example, some specialize in tuition payments and some in online reservations. The agency must also consider which gateway is compatible with its accounting system (e.g., banner for the universities and Datatel for the community colleges). While there are two gateway capture solutions available through OSC's master contract with STMS (PayPoint and First Data Global Gateway), an agency is not required to utilize either, just as it is not required to obtain POS terminals from STMS.

When is the PayPoint gateway service more appropriate to use than the Global Gateway or Common Payment Service solution?
PayPoint is a recommended solution for an agency that needs a "consumer interface" feature. Neither the First Data Global Gateway solution (formerly called YourPay) offered by STMS, nor the Common Payment Service gateway offered by ITS, has a web consumer interface feature. PayPoint is more suitable for agencies that have accounts receivable transactions that have been invoiced to a payer and can be authenticated online before being paid (either by the agency or by PayPoint). PayPoint is also suitable when the agency desires to offer bank draft (E-check) as a payment option, in addition to the credit card option.

Does PayPoint accommodate card-present transactions and MOTO?
Yes, in addition to accommodating web-initiated payments, PayPoint can also function as a "virtual terminal" solution, with the agency initiating the payments through the agency's Admin PC screen. This could be for walk-ins (card-present) or for mail orders / telephone orders (MOTO). The normal capture method would be for the agency personnel to key the cardholder data or check data (for bank drafts), on the Admin PC screen while connected to the PayPoint website in a secure session. PayPoint provides for a customer receipt to be printed, which can be provided to the payor (in person, or emailed). Card capture via a magnetic stripe reader connected to the agency's PC is an alternative to the agency personnel keying the card data onto the PC screen. For transactions entered through the Admin screen, the $.10 per transaction Consumer Interface fee does not apply.

Using a gateway as a virtual terminal does have certain PCI Data Security compliance implications, as cardholder data is being "processed" at the agency's location, via a device connected to the Internet. The degree of implications depends partially upon rather the PC is segmented from other agency servers or not. Agencies utilizing PayPoint as a virtual terminal must have the associated external IP addresses enrolled in TrustKeeper so that the external facing (public) IP addresses can undergo quarterly vulnerability scanning.

Are there other ways of utilizing PayPoint involving an API solution?
While PayPoint does offer an API (Application Programming Interface) solution hosted by the agency, it is not the recommended utilization of PayPoint for agencies, as it requires more agency website maintenance and greater PCI Data Security compliance implications. The Common Payment Service (CPS) available through the Office of Information Technology provides an API solution, using Cybersource middleware to process the transactions with SunTrust Merchant Services. While PayPoint and Global Gateway both offer an API solution hosted by the agency, the Common Payment Service normally can accommodate most agencies needing such a solution.

What type of technical knowledge must an agency have?
IT expertise that is needed by an agency will depend largely upon the type of interfacing of transaction data between the agency's transaction database and the PayPoint application. IT staff will be involved in both the setup of the upload process of open transactions to PayPoint (i.e., either Web Services or Secure HTTP); or 2) Batch XML (via Secure FTP site). Minimal technical knowledge is needed in developing the web portal using the consumer payment module. Knowledge of XML files, FTP file upload/download, and query strings are helpful when determining which methods of interfacing data (to and from PayPoint) are to be utilized. There are several methods of uploading and downloading of data to/from PayPoint available. The handling of data received from PayPoint (posting file) can either be interfaced or manually posted. A review of PayPoint's Integration Guides will give an agency an idea of the type of technical expertise needed.

How is the consumer payments website designed?
Using the Consumer Payments design toolkit (portal builder), for each payment application, the agency logs-on to PayPoint through the Admin site and creates its own webpage. The toolkit allows for the agency to use its own agency logo, pick a theme, fonts, colors, headers, footers, and establish rules for the particular payment. The site can be disabled as needed, such as to perform maintenance.

How does PayPoint handle the agency's logo?
The PayPoint application links to the agency's logo (gif or jpeg) maintained on a secure server maintained by either: 1) the State agency, or 2) First Data. If the URL link, which is provided during the setup, is not to a secure server (https), the consumers will get a security warning message when initiating payments. Unless the agency has a secure server to house the logo, the agency must provide the GIF or JPEG logo to First Data for hosting.

Are there any start-up fees for the agency?
There is a one-time setup fee of $1,000.00 payable by the subscribing agency. This fee is refundable to the participant, in the form of a credit, once its monthly transaction volume has reached 10,000 and has been maintained at that level for any 12 months (not required to be concurrent). Should there be any customized programming needed by an entity (for customized web development or customized file layout for summary bill presentment and authentication), the fee is $200 per hour, and requires a statement of work (SOW) to be completed.

Are there any on-going transaction fees?
STMS Amendment Number 2 contains the fee schedule. Transaction fees will vary based upon which of the two transaction interface options are utilized, and which additional features are utilized. The two basic fees per transaction fees that apply are: 1) Gateway transaction fee - $.20; and 2) Consumer Interface surcharge

fee - $.10. The $.10 surcharge does not apply for transactions entered via the agency's Admin site. If the Batch FTP interface feature is used, which requires authentication on PayPoint's website (instead of on the agency's website), an additional $.05 authentication/challenge fee would apply. These minimum basic per transaction fees for consumer initiated payments would therefore be either $.30 for HTTP Query String Web Service; or $.35 for Batch FTP. (Refer to chart on page 3).

What additional "other" on-going transaction fees could apply?
A "Summary Presentment Surcharge" fee of $.10 per transaction would apply if the agency wishes for payors to be displayed billing data (both paid and unpaid invoices) associated with the payor's ID. An "Enrollment" fee of $.02 per enrollment would apply if the agency wishes for the payors to be able to pre-enroll and maintain their own online profile (see below). The PayPoint fees would be in addition to any fees associated with processing card transactions through STMS, which involve interchange and assessment fees charged by the card brands.

Are fees for PayPoint services separate from fees for processing card transactions?
Yes. Services for fees associated with PayPoint will be invoiced by First Data Government Solutions, while services for processing card transactions will be invoiced by SunTrust Merchant Services (STMS).

Is there a payor Registration / Pre-Enrolled feature?
PayPoint offers the ability for payors to register, or pre-enroll in PayPoint, at either the agency or application level, providing the payors the ability to establish an online payor profile. For example, the payor's preferred method(s) of payment can be maintained on PayPoint. If used, the payor has the ability to view history of payments they have previously made, change the method(s) of payments, after logging in using their enrolled email address and password. However, this feature is not envisioned as being conductive to most agency operations, as it increases the agency's help desk interaction with users associated with their profile maintenance (e.g., forgotten passwords, change in bank accounts, change in card expiration dates, etc.). There could also be confusion if payors can change their profile on PayPoint, thinking they have also done it with the agency.

This feature may be appropriate if re-occurring payments are due from a payor (i.e., payment schedule is established). If the pre-enrollment feature is chosen, a separate application is recommended, separate from the application for payers not being pre-enrolled.

Are there any Interactive Voice Response (IVR) fees?
PayPoint accommodates IVR, but there is no perceived demand for this service. Initially, PayPoint will be used primarily for "card-not-present" transactions, and ACH bank drafts initiated through the Web, as well as via MOTO (mail order telephone order).

How are bank drafts (E-Checks) processed through PayPoint?
While card transactions are routed through STMS for collection and settlement, bank draft transactions (also referred to as E-Checks) are routed through TeleCheck, a business unit of First Data. TeleCheck functions as the ACH originating bank, with ACH debits being submitted against the payor's bank account, and the proceeds being credited to the agency's designated bank account. The agency's designated bank account normally is the same ZBA account the agency has with the State Treasurer for the settlement of its credit card transactions (at Wachovia for agencies).

Are there any fees associated with originating ACH bank drafts?
No, there are not any ACH related fees beyond the basic PayPoint per transaction fees. Should the payor select the bank draft option to initiate a payment (referred to as an "E-Check"), the agency avoids the interchange fees associated with processing merchant cards.

Can an agency elect to only offer the E-Check payment option for a particular application?
Yes, this may be appropriate when the average transaction amount for a particular application (or set of payers) is normally very large, and the agency does not want to incur the interchange fee associated with a card transaction. (Interchange fees are based on a percentage of the <u>amount</u> of a card transaction.)

When an open invoice transaction is displayed to a payer, can the payer change the amount field?
Any of the fields presented to a payer on the "Make Payment Screen" can be coded to be either editable or non-editable. Making the amount field editable would allow a partial payment.

When are funds credited to the agency's bank account maintained with the State Treasurer?
In the case of both card transactions and bank drafts (E-checks), funds are credited to the agency's dedicated bank account at Wachovia, one banking day after the transaction date. Exception is in case Amex or Discover are accepted, which has an additional one-day delay.

What tools are used to perform the funds reconciliation function?
The agency will utilize several online reporting tools to perform the reconciliation function. In the case of entities depositing funds with the State Treasurer, the dedicated sub-ZBA bank account assigned by the State Treasurer will be utilized to account for all funds received (as well as debits for returns and chargebacks) for the various transactions.

Funds will be received 1) from STMS credit card and debit card transactions; and 2) from TeleCheck for ACH (E-Check) transactions. A daily settlement will be received from each of these two sources on a daily basis, and credited to the agency's designated ZBA bank account established with the State Treasurer. Online tools to be utilized to view what is <u>expected</u> are ClientLine (for cards) and PayPoint Reports (for cards and E-Checks). The online tool to be utilized to view the funds <u>actually received</u> and credited to the bank account is Wachovia Connection.

On a daily basis, the agency's dedicated ZBA account at Wachovia will have the following transactions, for <u>each</u> application: 1) daily total of Visa/Mastercard transactions; 2) daily total of E-Check transactions; 3) individual card chargebacks; 4) individual bank draft returns. The net total of each day's transactions is swept from the agency's dedicated bank account to the State Treasurer's bank account, which is the amount the agency is to certify via OSC's Cash Management System (CMCS), using the agency's CIT number assigned by the State Treasurer. The agency is assigned one dedicated bank account for all applications, and has access to the bank account via the online Wachovia Connection system.

What are the tiered pricing fees contained in Amendment No. 2?
The basic PayPoint gateway transaction fee starts at $.20, which applies if the monthly transaction volume, for all agencies combined, is 50,000 transactions or less. The fee schedule allows for a tiered reduction should the monthly total transaction volume, for all agencies combined, exceed 50,000 transactions. OSC will notify the participating agencies should a new threshold be reached.

Does PayPoint accommodate a convenience fee being levied against a payor?
Yes. There are two options available: 1) Fee may be levied by the agency and collected by the agency; or 2) Fee may be levied by First Data Government Solutions (FDGS) and retained by FDGS. There are implications for levying a convenience fee, depending upon which card brands are accepted. For example Visa only allows a flat fee per transaction. The levying of convenience fees must be approved by OSMB and ITS pursuant to G.S. 66-58.12, even if the fee is retained by FDGS.

Does PayPoint accommodate Address Verification and/or Security Code Verifications?
Yes, AVS and CVV2 are accommodated. However, using AVS and CVV2 increases the rejection rate of valid card number and expiration date being submitted online. Should the agency authenticate each payor

(e.g., through a pre-assigned invoice number or vendor ID), these features could be waived, as the risk of a stolen card number being submitted is minimal. If the agency does not authenticate the payor, the CVV2 code verification feature should be used. There is an additional $.02 per transaction fee levied by STMS if AVS or CVV2 is utilized. Should the Discover Network Card be accepted, Discover levies a $.50 per transaction fee if AVS (for both street address and zip code) is <u>not</u> utilized for web payments. Other card brands do not have such requirement. The feature is selected when the Boarding Form is completed. Refer to OSC's document, <u>"Fraud Detection Services"</u> for more information.

What types of payments can be made through PayPoint?
Two types of merchant cards are typically accepted: 1) credit cards; and 2) Signature debit cards (with Visa/MC logo). In addition, ACH bank drafts (referred to as E-Checks) can be accepted.

What are and can PIN-less debit cards be accepted?
A PIN debit card is issued by a bank and generally requires authorization by the entering of a 4-digit PIN. The transaction results in the payment being deducted directly from the consumer's bank account.PIN debit cards bearing the mark of NYCE, STAR, and PULSE (and may or may not bear a Visa or MC logo) are eligible for a government to be accepted <u>without</u> having to acquire the 4-digit PIN, but a special enrollment is necessary through STMS. When taken in this manner, the card is referred to as a "PIN-less debit card" (not the same as a signature debit card). Selecting this feature is not typical for online payments. The feature can be added to the PayPoint during the initial setup (which can delay the implementation), or it can be added at a later date.

What card brands can be accepted?
All card brands can be accepted through PayPoint. Visa and MasterCard are eligible to be accepted as part of the contract with STMS. In order for American Express or Discover to be accepted, the agency must enroll in the services offered under master contracts that OSC has with those card brands. It should be noted that settlement of funds for American Express and Discover is two days instead of one day. The settlement of funds for ACH bank drafts (E-checks) is one day.

How is the authentication of payments performed?
All payments should be authenticated as being one that is an open transaction in the agency's accounts receivable database before the payor is allowed to initiate the payment. The authentication can be performed: 1) on the agency's website if the <u>HTTP Query String Web Services</u> interface option is utilized; or 2) on PayPoint's website if the <u>Batch FTP</u> interface option is utilized. PayPoint refers to the process as "challenge data." If the authentication (challenge) is performed at the PayPoint website, the agency must have uploaded the open transactions to PayPoint. In order to authenticate a payment, the payor should be prompted to enter at least two elements associated with an open transaction, such as invoice number (or license number) and amount of the obligation. These elements are established when the payment application is setup. The payor will normally be aware of the two challenge elements as a result of an invoice having previously been submitted to the payor. If the payor does not enter the appropriate challenge data, the open transaction cannot be retrieved and displayed, and the payment cannot be initiated, with an error message being displayed back to the person.

What are the two batch upload methods available to send a file to PayPoint?
- "Manage Uploads" option under "Data Management" through the Admin Site – User can browse to locate a file and then submit. Recommended for smaller files under 100 MB.
- Secure FTP site – Recommended for larger files. Requires file to be encrypted. Transmission can be manual or automated.

What are the stages of a payment being made online by a payer?
There are five stages of a transaction, with each stage having a unique screen:
- Challenge Screen – Payment data entered (On agency's website instead of PayPoint if Query String option utilized)
- Bill Preview Screen – If challenge data matches, the invoice to be paid is displayed
- Make Payment Screen – The payer selects the method of payment. Any additional info the agency wishes to capture, can also be required to be entered by the payer.
- Payment Preview Screen – Displays payment data entered, and allows payer to go back to the Make Payment screen to make any corrections
- Payment Complete Screen – Once the payment has been processed, the Payment Complete screen displays the transaction results and will display a confirmation number, if successful. If a transaction is not successful, this screen will display payment rejection reasons. Upon exiting the Payment Complete screen, the payer is redirected back to the agency's website.

For each of the above screens on PayPoint, the agency designs the screen, by placing text instructions in both the header and the footer. There is also a "Page Footer" which shows at the bottom of all pages. Contained here are links to the agency's website containing info such as, "Contact Us" and "Privacy Statement."

Is the payer provided a confirmation of the payment?
Yes, upon successfully initiating a payment online, the payer will be provided a confirmation screen, which can be printed. Additionally, for payments entered by the agency through the Admin site, the agency's administrator can generate a confirmation which can be emailed or mailed to the payer.

Can an email confirmation be sent to the payor for an online payment?
The payer is provided a confirmation screen which he/she can print. In addition, an email confirmation can be sent, but only if the "registration/enrollment" feature is utilized.

What type of information is passed from PayPoint to the agency upon completion of a payment?
For both uploading interfacing options (query string or Batch FTP), information pertaining to payment results is available to the agency via a "posting file," generally the next business day. The posting file is in a comma delimited format and can be: 1) downloaded via the agency's admin screen; or 2) automatically downloaded from an FTP site. The posting file is available in various formats from the Admin site. If downloaded from the FTP site, the file is an ANSII text file. Information on the posting file has data that can be used to update the agency's A/R database. See page 128 of the PayPoint Merchant Integration Guide for specifications on the "posting file." In addition, the agency can create customized reports using the Search/Report feature and export the file in an Excel format.

If the HTTP Query String (Web Service) interface option is utilized, an electronic response can be sent to the agency real time upon the completion of a payment transaction. If the FTP Batch interface option is utilized, real-time updating is not the norm, as updating is performed by downloading a posting file on a scheduled basis. However, for the FTP Batch option, a real-time update <u>can</u> be sent to the agency after each payment using a custom "Post Authorization plug-in" module, where a response would be sent directly to the agency. This would allow for the agency to update its records immediately if waiting to download the "posting file" is not acceptable. The Post Authorization plug in incurs additional customization costs.

What is the Reference field?
The reference field is a 254 character field associated with a payment transaction that can contain information about a payment beyond the standard information fields associated with a transaction. The reference field can contain multiple elements of information to identify the transaction. For example, it can contain invoice number, license number, or other fields that the payor has been prompted to enter on a

capture screen. The reference field is contained on the posting file downloadable from Paypoint, which the agency can use to map to its database.

How are payments that are in the A/R database cleared if a payor pays the agency directly by check instead of via PayPoint?
If the Batch FTP option is being utilized (where PayPoint performs the authentication function), the agency would update the records within PayPoint by sending updated files to PayPoint on a daily basis with current status information. The new file could either delete the previously submitted file, or mark the item with a new status of paid.

What are the three hierarchy levels associated with a payment?
A payment is processed/stored/search under the following hierarchy: 1) Site; 2) Agency; 3) Application. The "site" will always be ""NCOSC –NC Office of State Controller." The "agency" will always be (your agency). There can be multiple "applications" under (your agency), with each application being assigned a three digit number. You will only have access at the Agency level, and can assign specific access to individual applications under the Agency, based on the roles and access levels needed by your staff.

How are transactions identified in PayPoint?
Within each payment application, a newly created transaction (primary payment) is initially assigned a "transaction ID." Each primary payment transaction may have several subsequent actions associated with that that transaction, such as, cancellation, or chargeback. Each action (payment type) associated with the transaction ID has its own unique "confirmation number." Upon viewing a transaction ID, you can drill down to view each "action" associated with the payment by using the confirmation number.

Do transaction records have different status codes?
Yes, a transaction could be "successful - payment pending," or "settlement complete." Once a payer initiates a payment, PayPoint accumulates all payments and submits them for payment (either to STMS for cards or to TeleCheck for E-Checks) at an established nightly cut-off time. Up to the point the transaction is settled, the transaction can be canceled. The cut-off time should be prior to 9:00 p.m., and is established when the application is set up.

Can transactions be refunded?
To initiate a refund, there must be a previously entered transaction, either a card transaction or an E-Check transaction. A refund entered against a previous card transaction (which may be for the full amount or a partial amount) initiates a credit back to the card, and results in funds being transferred from the agency's bank account to the cardholder's card account. A refund entered against a previous E-Check transaction (which normally is for the full amount) does not result in the movement of funds, as it only results in the change of the transaction's status. If the agency learns of an E-Check return from the bank, the agency can log on to the Admin site and record the transaction as a return. E-Check returns will are associated with bank drafts returned due to either the bank account that was provided is invalid, or the payer's bank account had insufficient funds.

What is a chargeback?
Chargebacks only apply to card transactions. Chargebacks entered by the agency only results in the change of the transaction status, not the movement of funds. A chargeback entry is used when the agency learns that STMS has debited the agency's bank account, for a previously settled card transaction.

Can duplicate payments be prevented?
During an application's setup, the system can be coded to not allow duplicate payments within a certain time frame.

Can a web payer's IP address be viewed?
Yes, each transaction has a "source ID." In the case of a web payment, this would be the payor's IP address, which could be useful in detecting fraud transactions.

Are multiple languages supported?
Currently, both English and Spanish are supported.

How does the PCI Data Security Standard apply to PayPoint?
STMS Amendment Number 2 has a stipulation that requires First Data to acknowledge that as a service provider, it is responsible for the security of cardholder data it possesses, as required by Requirement 12.8 of the DSS. How the agency uses PayPoint will determine which Self Assessment Questionnaire (SAQ) the agency must complete. If the Admin screen will never be used by the agency to initiate card payments on behalf of a payer (functioning as a virtual terminal) vulnerability scanning is not required, and SAQ-A applies.

Agencies utilizing PayPoint as a virtual terminal (entering card transactions via the Admin screen) must have the associated external facing (public) IP addresses enrolled in TrustKeeper so that the IP addresses can undergo quarterly vulnerability scanning. The completion of SAQ C is required if: 1) data is not stored in electronic format; and 2) the PC is a stand-alone-terminal not connected to any other system. Otherwise, the completion of SAQ-D is required.

In the State's setup structure, who functions as the Corporate Site?
The Office of the State Controller (NCOSC) functions as the corporate site, and each agency functions as a participant under the site. Each agency can then have multiple payment applications.

How does the administrator function work?
The OSC has an administrator with the ability to setup an administrator at each agency, providing him/her certain administrator rights. Each agency's administrator then has the ability to: 1) set up applications; and 2) set up users within the agency. The administrator also assigns roles to users.

What types of reports are available?
There are nine standard reports available. In addition, an agency can create customized reports using templates. The reports are available in various formats, including cvc and XML. The reports can be exported to Excel if desired.

Who is responsible for the help desk function?
FDGS provides help desk services to an agency regarding the operation of PayPoint. However, each agency is responsible for maintaining its own help desk to deal with problems encountered by payers.

Does an agency have to execute an agreement in order to subscribe to PayPoint?
The agency must be a participant under the OSC's master contract with STMS for merchant card processing services, which requires the agency to have previously executed a "Schedule E – Agency Participation Agreement." The revised Schedule E has a separate section at the end which the agency would have to complete in order to subscribe to the PayPoint optional service. An agency may re-execute Schedule E if it is an existing participant, and now desires to subscribe to the PayPoint service.

Does the agency have to establish a separate merchant number for card transactions?
Yes, a separate merchant number is needed for each application that will accept cards, as merchant numbers are normally associated with a particular capture method and are needed to identify the Visa/Master card daily settlements for a particular application. Merchant numbers do not apply to E-Check transactions, but a TeleCheck number is assigned to each application, similar to a merchant number.

What is the implementation process?
The implementation phases include: 1) Analysis of features/interfaces to be utilized; 2) complete PayPoint Boarding form 3) registration and setup; 4) interface development; 5) testing; 6) certification; and 7) production. Once the interface option is chosen (query string or Batch FTP), there is a boarding form that an agency must complete upon enrolling. A separate boarding form is to be completed for each "payment application" the agency will be accepting online. An agency will typically have multiple payment applications (e.g., license renewal, permit fees, fines, etc.).

What is the UAT Region?
After selecting the upload interface for an application, and completing the Boarding Form, the PayPoint project manager will setup the application in PayPoint's "User Acceptance Test" (UAT) region. The application will be similar to what will eventually be in the Production Region, but not necessarily the same. The UAT region will allow the agency to perform three modes: 1) Testing; 2) Certification; and 3) Production. The "production mode" is not really true production, as it is within the UAT Region.

What is the Production Region?
After performing all three modes within the UAT Region, the agency will be setup in the Production Region, based on the Boarding Form completed by the agency, but modified according to any necessary changes identified necessary while testing in the UAT Region. The same three modes (testing, certification, and production) will be performed in the Production Region. However, during the certification mode, live $1.00 transactions will be initiated against real card and bank accounts.

Does the International ACH Transaction (IAT) Rules apply to the E-Check transactions?
Yes. Since the agency will be accepting E-Check transactions, which is an Automated Clearing House (ACH) debit online, the agency must perform its due diligence efforts to prevent the website from being used as a means to originate ACH transactions against a bank account funded with moneys from a foreign bank. The agency must include language in its website's Privacy Policy to address the IAT rules. See the Sample IAT Privacy Statement.